UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,165	03/17/2004	James D. Gersten	ELYN/10	4146

26875 7590 12/12/2007

WOOD, HERRON & EVANS, LLP
2700 CAREW TOWER
441 VINE STREET
CINCINNATI, OH 45202

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
12/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/802,165	GERSTEN ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on October 22nd, 2007. Claims 11 and 30 have been amended. Claims 1-37 are pending and have been considered below.

Claim Objections

2. The amendment to claims 11 and 30 filed on October 22nd, 2007 has been considered and effectively overcome the previous claim objections. Therefore, the previous claim objections have been withdrawn.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Applicant asserts that the claims is directed to something very physical –"transmission medium" would include, e.g., network connections. The claim thus is directed to something very, physical - a signal bearing medium -- and not merely to "energy" as the Examiner seems to posit." The examiner respectfully disagrees.

Applicant is right, the claim is "a signal bearing medium" that carries program code. However, this "signal bearing medium" can be transmission type media such as digital and analog communication links" as disclosed on page 12 of the specification. Therefore, taking this description of signal bearing medium, the claim is considered to be directed to nonstatutory subject matters. Accordingly, the rejection is sustained.

Response to Arguments

4. Applicant's arguments filed on October 22nd, 2007 have been fully considered but they are not persuasive.

Applicant argues on page 13 of the response that " A "secure network connection"• is recited in each and every independent claim." As such, Applicant contends that "Michael is not proposing the use of a secure network connection to communicate emails containing banners" Emphasis added. See response at page 14. The examiner respectfully disagrees.

Contrary to Applicant's assertion, Michael's disclosure does relate to a secure network connection. Michael recognizes the need for a secure network connection. For example, in paragraph [0027], Michael discloses, "Although new guidelines and regulations may be created, it seems that it is impossible to prevent unsolicited commercial bulk email or force the use of spam identifiers. Furthermore, in paragraph [0029], Michael discloses," The invention also includes method for encrypting and authenticating the code set, tags and other such distinguishing means in order to prevent or reduce the likelihood of non-authorized use of its standards and code set. See also paragraphs [0056], [0057], and [0094]. Accordingly, it is submitted that Michael meets/discloses the claims "Secure network connection". It should also be pointed out that Benninghoff also relates to a secure network connection. See paragraphs [0014], [0121], and [0125].

It is also noted that Applicant disagrees with the examiner for relying on Dye patent for showing the use of an https socket layer for data communication. According to Applicant, the Michael system is not compatible with https protocol delivery since" using https protocol delivery would render the Michael client unusable as "an add-on to or ..." The examiner respectfully disagrees.

First, as noted above, Michael does disclose a "secure network connection". Thus, Michael system would be compatible with https protocol delivery of Dye.

In the overview of the invention, paragraph [0003], Michael describes that, "the invention's email system can be seen as a "proprietary" email system over internet transport email system, where additional proprietary standards and code sets are used to distinguish and to provide special handling for its emails from the general emails. The email distinguish methods will used for a variety of types of emails - -such as opt-in or permission-based emails in order to route them to their respective "opt-in" destination folders or interfaces."

Furthermore, in paragraph [0034], Michael discloses, "It is an objective of the invention to provide method and systems for an email system over the internet that is accessible to only senders and their emails using the system's code sets and standards."

Therefore, the combination of Dye patent is NOT a contradiction to the purposes and design of the Michael system.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 16, 18 are rejected under 35 U.S.C. 102(b) as being anticipated by **Michael** (US 2002/0188689).

Claim 16: **Michael** discloses a method for secure electronic mail transfer comprising:

i. Generating at a local computer using a non-browser application configured for electronic transmission that includes an electronic mail analogous interface, an encrypted package comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107);

ii. And transmitting from the local computer the package over a secure network connection over the public Internet (the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key (page 12, paragraph 161).

Claim 18: **Michael** discloses a method for secure electronic mail transfer as in claim 16 above, and further discloses a step of communicating the package to the addressee (if sender is authenticated, the email message will be delivered to recipient's mailbox and will be accessible to recipient's email application) (page 12, paragraph 164)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-10, 12, 13, 17-21, 23-29, 31, 33-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Michael** (US 2002/0188689) in view of **Benninghoff** (US 2002/0091782).

Claim 1: **Michael** discloses a method for secure electronic mail transfer comprising:

i. Generating a package using a non-browser application on a local computer, the package configured for electronic transmission that includes an electronic mail analogous interface, file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107);

ii. Communicating the package from the local computer to a secure server over a secure network connection over the public Internet (If the email has predefined identifiers the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key) (page 12, paragraph 161);

iii. Communicating the package to the addressee (if sender is authenticated, the email message will be delivered to recipient's mailbox and will be accessible to recipient's email application) (page 12, paragraph 164);

iv. Decrypting the package (the receiver can decrypt the email using sender private key) (page 12, paragraph 161);

v. And displaying the package to the addressee (the recipient's destination application recognizes the header bearing email and displays such) (page 9, paragraph 07).

Michael does not disclose that the package is stored at the server. However, **Benninghoff** discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to **Michael**'s teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 17: **Michael** discloses a method for secure electronic mail transfer as in claim 16 above, but does not explicitly disclose that the package is stored at the server. However, **Benninghoff** discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to **Michael**'s teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 21: **Michael** discloses an apparatus for secure electronic mail transfer comprising:

i. A computer (page 1, paragraph 6);

ii. A program code in communication with at least one of the local and server computers, the program code configured to generate a package using a non-browser application on the local computer, the package being configured for electronic transmission that includes an electronic mail analogous interface, file data and an address associated with an addressee having a public electronic mail account (the present invention,

graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), the program code being further configured to communicate the package from the local computer to the secure server over the secure network connection (If the email has predefined identifiers the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key) (page 12, paragraph 161), and to store the package at the server in association with the electronic mail account of the addressee, the program code being further configured to decrypt (the receiver can decrypt the email using sender private key) (page 12, paragraph 161) and communicate the package to the addressee the recipient's destination application recognizes the header bearing email and displays such) (page 9, paragraph 07).

Michael does not disclose: the package is stored at the server; a server computer;

However, **Benninghoff** discloses a method of verifiably transmitting an electronic package, which further discloses

> A server computer configured to communicate with the local computer over a secure network connection (figure 1);
>
> And a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125).

Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step storing the electronic package at the server to **Michael**'s teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claims 2, 23: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and **Michael** further discloses that the package is encrypted at the local computer of a sender (the sender can encrypt the email using their public key) (page 12, paragraph 161).

Claims 3, 24: **Michael**, and **Benninghoff** disclose a method and system for secure electronic mail transfer as in claims 2 and 23 above, and **Michael** further discloses that the step of encrypting the package at the local computer of the sender further includes using a public key to encrypt the package (the sender can encrypt the email using their public key) (page 12, paragraph 161).

Claims 4, 25: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and **Michael** further discloses that the step of decrypting the package further includes using a private key associated with a public key previously used to encrypt the package (the receiver can decrypt the email using sender private key) (page 12, paragraph 161).

Claims 5, 26: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and **Benninghoff** discloses a method and apparatus of verifiably transmitting an electronic package, which further discloses a step of storing the package as a draft package at the local computer prior to communicating the package to the secure server (the invention provides a system and method where any person may caused to be transmitted electronically files in electronic format and register electronically with PoS-e the time, date, file size, sender, and recipient of said transmission and provide that a duplicate of the transmitting message be stored on PoS-e's server for a designated period of time) (page 4, paragraph 60). Therefore, it would have been obvious for one having ordinary skill in the art at

the time the invention was made to add a step of storing the package as a draft to **Michael**'s teaching. One would have been motivated to do so in order to allow the user to complete the package at a later time.

Claims 6, 27: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and **Benninghoff** discloses a method and apparatus of verifiably transmitting an electronic package which further discloses a step of causing the addressee to be notified of the package using the public electronic mail account (the server sends an email notification to the recipient indicating that an electronic package addressed to the recipient is available on the server) (page 8, paragraph 133). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of notifying the addressee in **Michael**'s teaching. One would have been motivated to do so in order to allow the addressee to access the package.

Claims 7, 28: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and **Michael** further discloses that communicating the package to the addressee further includes communicating the package using at least one of the secure network connection and a second secure network connection (the sender signs the emails using their private key, the recipient server can verify the sender information the email using sender's public key) (page 12, paragraph 161).

Claim 8: **Michael**, and **Benninghoff** disclose a method for secure electronic mail transfer as in claim 1 above, and **Benninghoff** discloses a method and apparatus of verifiably transmitting an electronic package which further discloses a step of configuring the interface to be responsive to user input (at step 142, via the sender's client-side application, the system display various PoS-e services that may be selected by sender as is appropriate to his circumstances) (page 7, paragraph 126). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of getting user input to **Michael**'s teaching. One would have been motivated to do so in order to allow the user to enter or change data in the package.

Claims 9, 29: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, and **Benninghoff** discloses a method and apparatus of verifiably transmitting an electronic package, which further discloses a step of configuring the interface to display a status of the package (Figure 27). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step of configuring the interface to display status of the package to **Michael**'s teaching. One would have been motivated to do so in order to allow the sender to determine when the package was delivered.

Claim 10: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claim 1 above, and **Michael** further discloses a step of adding additional file data to the package (hyperlinks or other resources

are attached to the header, including a typical email body) (page 9, paragraph 107).

Claim 12: **Michael**, and **Benninghoff** disclose a method for secure electronic mail transfer as in claim 1 above, and **Benninghoff** discloses a method of verifiably transmitting an electronic package which further discloses a step of downloading the package from the secure server (the recipient download the contents of the electronic package that was prepared and transmitted by the subscriber) (page 8, paragraph 134). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step downloading the package to **Michael**'s teaching. One would have been motivated to do so in order to allow the receiver to access the package.

Claims 13, 31: **Michael**, and **Benninghoff** disclose a method for secure electronic mail transfer as in claims 1 and 21 above, and **Benninghoff** discloses a method of verifiably transmitting an electronic package which further discloses a step of automatically downloading the package from the secure server (the server presents the recipient with a download page like that shown in fig 11. which allows the recipient to elect delivery of the electronic package by either downloading it with a java applet, by downloading directly, or by receiving it as an encrypted email attachment) (page 8, paragraph 134). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add a step downloading the package to **Michael**'s teaching. One would

have been motivated to do so in order to allow the receiver to access the package.

Claim 19: **Michael** discloses a method for secure electronic mail transfer comprising:

i. Receiving over a secure network connection over the public Internet a package, using a non-browser application that includes an electronic mail analogous interface, the package configured for electronic transmission and comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107),

ii. Decrypting the package (the receiver can decrypt the email using sender private key) (page 12, paragraph 161);

iii. And displaying the package to the addressee (the recipient's destination application recognizes the header bearing email and displays such) (page 9, paragraph 07).

Michael does not disclose that the package is stored at the server.

However, **Benninghoff** discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to **Michael**'s teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity

Claim 20: **Michael** discloses a method for secure electronic mail transfer comprising:

i. Generating a package for electronic transmission using a non-browser application that includes an electronic mail analogous interface (the present invention, graphical banner like display is used in lieu of the current arts inbox for text-based header for email. It is transported over the typical email protocols and displayed at the destination client. It can

be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107);

ii. Encrypting the package (the sender can encrypt the email using their public key) (page 12, paragraph 161);

iii. Communicating the package from the local computer to a secure server over a secure network connection over the public Internet wherein the package is stored at the server and communicated to an addressee (If the email has predefined identifiers the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key (page 12, paragraph 161);

Michael discloses neither that the package is stored at the server nor communicating the delivery status of the package. However, **Benninghoff** discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and

use in generating the electronic certificate of service) (page 7, paragraph 125), which further discloses a step of causing the addressee to be notified of the package using the public electronic mail account (the server sends an email notification to the recipient indicating that an electronic package addressed to the recipient is available on the server) (page 8, paragraph 133). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server and a step of notification of the package status to **Michael**'s teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity

Claim 33: **Michael** discloses an apparatus for secure electronic mail transfer comprising:

i. A computer (page 1, paragraph 6);

ii. And program code in communication with the computer, the program code using a non-browser application and including an electronic mail analogous interface configured to receive from a remote computer over a secure network connection over the public Internet an encrypted package comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email

protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), the program code being further configured to store the package in association with an electronic mail account of the addressee and to communicate the package to the addressee (If the email has predefined identifiers the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key (page 12, paragraph 161).

Michael does not explicitly disclose that the package is stored at the server. However, **Benninghoff** discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to **Michael**'s teaching. One would have

motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 34: **Michael** discloses an apparatus for secure electronic mail transfer comprising:

i. A computer (page 1, paragraph 6);

ii. And program code in communication with the computer, the program code configured to receive over a secure network connection over the public Internet a package generated using a non-browser application that includes an electronic mail analogous interface, the package being configured for electronic transmission and comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), wherein the package has been stored remotely at a secure server, the program code further configured to decrypt and display the package

(the receiver can decrypt the email using sender private key) (page 12, paragraph 161).

Michael does not explicitly disclose that the package is stored at the server. However, **Benninghoff** discloses a method of verifiably transmitting an electronic package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to **Michael**'s teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 35: **Michael** discloses an apparatus for secure electronic mail transfer comprising:

i. A computer (page 1, paragraph 6);

ii. And program code in communication with the computer, the program code configured to generate a package using a non-browser application that includes an electronic mail analogous interface, the package being configured for electronic transmission (the present invention, graphical banner like display is used in lieu of the current arts

inbox for text based header for email. It is transported over the typical email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body). (page 9, paragraph 107), the program code further being configured to encrypt the package and to communicate the package from the computer to a secure server over a secure network connection over the public Internet (the sender can encrypt the email using their public key) (page 12, paragraph 161), wherein the package is stored at the server and communicated to an addressee, wherein the program code is further configured to communicate a confirmation of delivery status of the package from the secure server to the non-browser application at the local computer via a secure network connection over the public Internet.

Michael does not explicitly disclose:

The package is stored at the server;

The program code is further configured to communicate a confirmation of delivery status of the package from the secure server.

However, **Benninghoff** discloses an apparatus of verifiably transmitting an electronic package, which further discloses a step of storing the package at the

server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125) and a step of communicating the status of package (the server sends an email confirmation to the sender indicating that the electronic package has been received by the server and is pending delivery to the recipient) (page 8, paragraph 133). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server and a step of notifying the sender to **Michael**'s teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 36: **Michael** discloses a program product for secure electronic mail transfer comprising:

i. Program code in communication with at least one of a local and a server computer, the program code configured to generate a package using a non-browser application that includes an electronic mail analogous interface on the local computer, the package being configured for electronic transmission comprising file data and an address associated with an addressee having a public electronic mail account (the present invention, graphical banner like display is used in lieu of the current arts inbox for text based header for email. It is transported over the typical

email protocols and displayed at the destination client. It can be created at an online web interface where templates of appropriate sizes, and styles are provided to the user. User can stylize the header in a variety of ways. If desired, the sender name, the name of the intended recipient, hyperlinks or other resources are attached to the header, including a typical email body) (page 9, paragraph 107), the program code being further configured to communicate the package from the local computer to the secure server over a secure network connection (the email will be checked for authentication information. The authentication part in the previous example is using company name and digital signature. The sender signs the email using their private key, the recipient server can verify the sender information the email using sender's public key (page 12, paragraph 161), and to store the package at the server in association with the electronic mail account of the addressee, the program code being further configured to decrypt and communicate the package to the addressee package (the receiver can decrypt the email using sender private key) (page 12, paragraph 161);

ii. And a signal bearing medium bearing the program code (the invention system may also be considered to be implemented as a computer readable storage medium) (page 1 paragraph 7).

Michael does not explicitly disclose that the package is stored at the server. However, **Benninghoff** discloses a method of verifiably transmitting an electronic

package which further discloses the a step of storing the package at the server in association with the electronic mail account of the addressee (the system stores the electronic package and particulars related to the transmission thereof for later delivery and use in generating the electronic certificate of service) (page 7, paragraph 125). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to add the step of storing the electronic package at the server to **Michael**'s teaching. One would have motivated to do so in order to allow the package to be delivered at a later time, such as during a period of low activity.

Claim 37: **Michael**, and **Benninghoff** disclose a program for secure electronic mail transfer as in claim 36 above, and **Michael** further discloses that the signal bearing medium includes at least one of a recordable medium and a transmission-type medium (such computer program is preferably stored on a storage media or device readable by general or special purpose programmable computer) (page 1, paragraph 7).

9. Claims 11, 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Michael** (US 2002/0188689) and **Benninghoff** (US 2002/0091782) in view of **Maxwell** (US 5805810).

Claims 11, 30: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, but do not disclose a

step of including a PCL file within the file data. However, **Maxwell** discloses a method and apparatus for converting electronic mail to a postal mail at the receiving station which further disclose the use of a (Printer Control Language (PCL) file within the file data (if the email contains sufficient information to generate a mail object, message validator provides the generated mail object to the print queue processor executing in the print server. The print queue processor then prints the mail object as postal mail) (column 5, lines 50-60). It would have been obvious to one ordinary skill in the art at the time the invention was made to modify the combined method, and apparatus of **Michael**, and **Benninghoff** such as to add the step generating PCL file. One would have motivated to do so in order to ensure delivery of the package.

10. Claims 14, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Michael** (US 2002/0188689) and **Benninghoff** (US 2002/0091782) in view of **Montville et al** (US 6356937).

Claims 14, 32: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, but do not disclose a step of compressing at least a portion of the package. However, **Montville** discloses a similar method and apparatus, which further discloses a step of compressing at least a portion of the package (the user is given control over whether or not to compress the file size of each outgoing attachment to a message) (column 3, lines 65-67). It would have been obvious to one ordinary

skill in the art at the time the invention was made to modify the combined method, and apparatus of **Michael**, and **Benninghoff** such as to add the step of compressing at least portion of the file. One would have motivated to do so in order to decrease the bandwidth needed to transmit the package.

11. Claims 15, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Michael** (US 2002/0188689) and **Benninghoff** (US 2002/0091782) in view of **Dye et al** (US 2005/0114658).

Claims 15, 22: **Michael**, and **Benninghoff** disclose a method and apparatus for secure electronic mail transfer as in claims 1 and 21 above, but do not explicitly disclose the use of https socket layer connection. However, **Dye et al** discloses a remote web site security system, which further disclose the use of a secure Https layer (figure 1). It would have been obvious to one ordinary skill in the art at the time the invention was made to modify the combined method, and apparatus of **Michael**, and **Benninghoff** such as to use a secure https connection. One would have motivated to do so in order to prevent unauthorized access to the package by third parties.

Conclusion

12. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Tuesday November 12th, 2007

Kambiz Zand
Supervisory Patent Examiner